SECURE360 conference

KELLEY P. ARCHER, CISSR

ID THEFT PREVENTION - *YOU ARE VULNERABLE!*

TUESDAY, MAY 14, 2013 - 1 PM

WELCOME TO SECURE360 2013

- Don't forget to pick up your Certificate of Attendance at the end of each day.

- Please complete the Session Survey front and back, and leave it on your seat.

- Are you tweeting? #Sec360

Identity Theft Prevention

Kelley P. Archer, CISSR

Spring 2013

Agenda

- What is Identity Theft
- Who wants my information & why
- How do they get my information
- What to do if I think I'm a victim
- How to protect myself
- Questions

What is Identity Theft

- Fraud attempted or committed using your information without authority
  - 13 straight years ID Theft is top complaint
  - More than just stealing your credit card information
  - Thieves use your information to become you, i.e. social security number, account information, medical information, credit information
  - Posing as YOU ruining your good credit rating and/or you get arrested

What is Identity Theft – cont.

- 1 in 3 families in U.S. have been a victim; 1 in 4 people have been victim
- Cybercrime hits nearly 3 out of 4 online users in US
- Average out of pocket lost – up from $387 to $631, 60% increase
- Internet Crime up 50% in 2012
- Avg. number of hours spent repairing ID = 330
- A crime is committed and YOU are arrested
- YOU are guilty until YOU prove you're innocent
  - 12% of victims have warrants issued in their name
    - Woman returning from Jamaica vacation
    - Arrested for Federal Warrant – bank robbery suspect jumped bail

What is Identity Theft – cont.

- 70% of victims have trouble removing negative information
- Nearly 12 million people affected
  - 3 million of deceased
- Over 300 ID fraud related arrests made every year
- Over 300 of ID thieves end up in prison
- 11% of U.S. adults paid for fraudulent products and services in 2011
- Internet most-reported source for fraudulent solicitations

What is Identity Theft – cont.

- iPhone and Android users higher risk for ID fraud
  - 7% of smartphone owners are victims
  - 1/3 of general public
- 2012 increased fraud by 13%
  - LinkedIn, Google+, Twitter and Facebook users had the highest incidence of fraud although there is no proof of direct causation
- Nearly 12 million people affected
  - 3 million of deceased

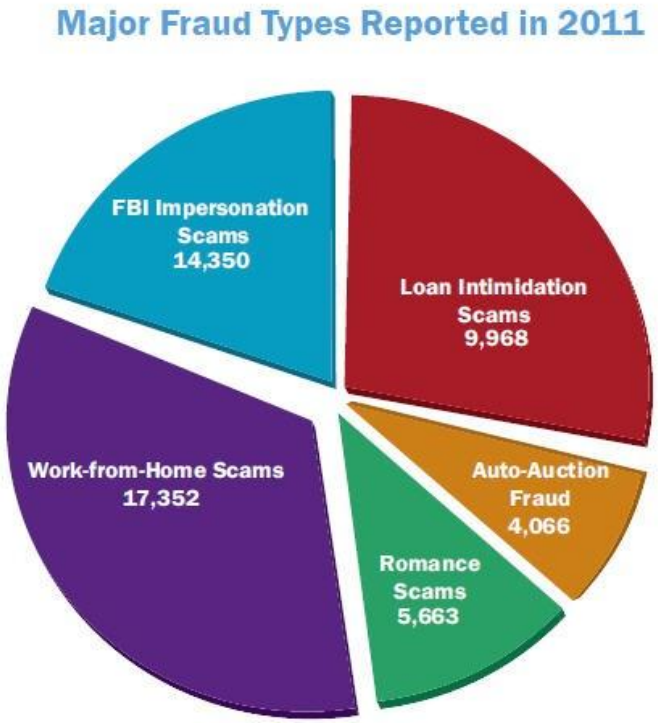
Who wants my information & why?

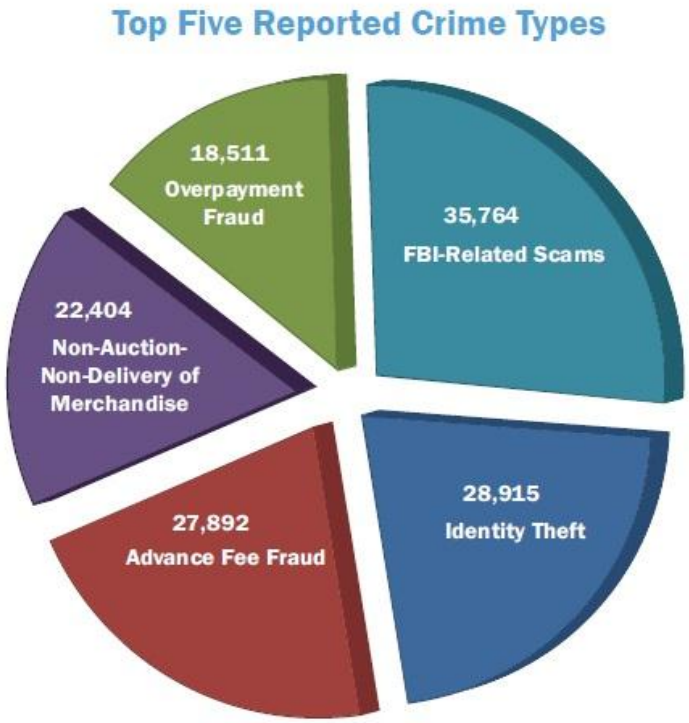
- Hackers
  - Average profile = male, single, age 10-14, loner, low self-esteem, few friends
  - The challenge of getting access to information
  - Ego, Pride among thieves, $$$
- Thieves & Foreign entities
  - China, North Korea, India, Russia, Iran, Africa nations, South America, Mexico, etc.
  - $$$$$$$

How do they get my information

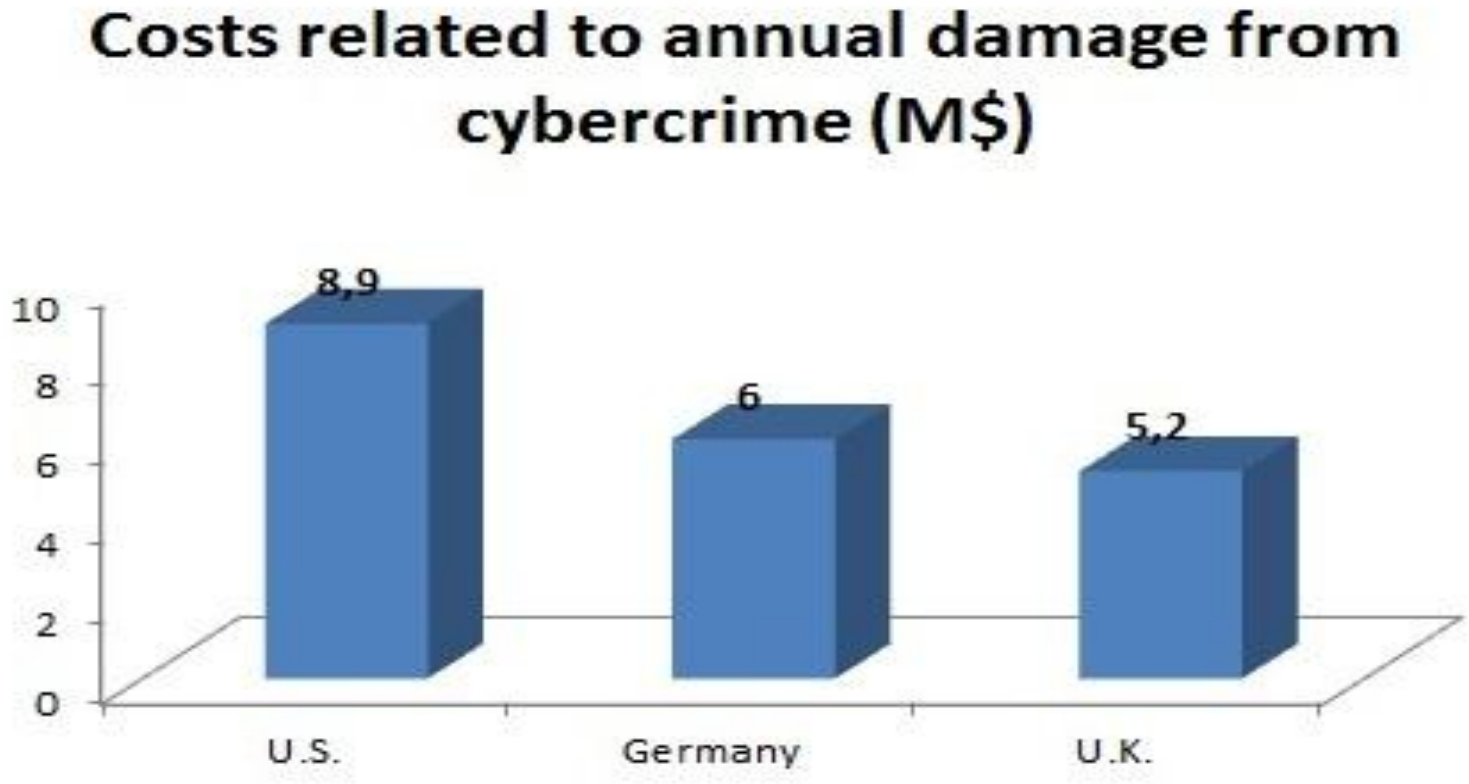
- **High Tech = 15%**
  - **Phishing/Hacking Techniques** - Emails & collecting information from unsecured web sites on the Internet
    14% of these are successful in obtaining information
  - **Spyware –** monitors and records personal information keyed directly into actual sites.
  - **Skimming** - Steal credit card information using special scanning devices
  - **Social Engineering** - posing as someone who think you can trust - bank, credit card company, meter reader, charity provider
  - **Fax machines** – Connect to fax machine and access computer
- **Low Tech = 85%**
  - **Stealing wallets/purses** – 50% of us carry our SSN card
  - **Mail theft** – 1in 80 families has mail stolen each year
  - **Dumpster Diving** - going through your trash, over 40% of unsolicited credit cards thrown away intact
  - **Wayward Receipts** – partial credit card numbers/printed on

How do they get my information





ID THEFT COST



HOW DO THEY GET MY INFORMATION

SAMPLE OF PHISHING EMAIL

Phishing e-mails will contain some of these common elements: (view screen capture above from Eudora)

1. *The "From Field" appears to be from the legitimate company mentioned in the e-mail. It is important to note, however, that it is very simple to change the "from" information in any e-mail client. While we're not going to tell you how, rest assured it can be done in a matter of seconds!*

2. *The e-mail will usually contain logos or images that have been taken from the Web site of the company mentioned in the scam e-mail.*

3. *The e-mail will contain a clickable link with text suggesting you use the inserted link to validate your information. In the image you will see that once the hyperlink is highlighted, the bottom left of the screen shows the real Web site address to which you will go. Note that the hyperlink does NOT point to the legitimate Citibank Web site URL.*

In this instance, the text you click is "here", However, this may also state something like "Log-in to Citibank" or "www.citibank.com/secure" to be even more misleading. This clickable area is only text and can be changed to anything the sender wants it to read.

How do they get my information

Sample of Phishing email

From: Capital One [CapitalOne@online.com] Sent: Wed 4/16/2008 9:
To:
Cc:
Subject: Capital One will never ask for your PIN

Dear Capital One Customer,

During our regularly scheduled account maintenance and verification procedures,
we have detected a slight error in your account information.
To securely confirm your personal information please click on the link bellow:

https://onlinebanking.capitalone.com/CAPITALONE/Enrollment.aspx?03942561

Confirm Your Capital One Account now to enjoy the benefits of
online banking and finance to avoid identity theft and fraudulent activities on
your account.

Note: We will be upgrading our yearly SSL EncryptedServer to prevent fraudulent activity.

HOW DO THEY GET MY INFORMATION

SAMPLE OF PHISHING EMAIL

Message Page 1 of 1

From: Internal Revenue Service [mailto:admin@irs.gov] Sent: Wednesday, March 01, 2006 12:45 PM To: john.doe@jdoe.com Subject: IRS Notification - Please Read This .

After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of $63.80. Please submit the tax refund request and allow us 6-9 days in order to process it.

A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline.

To access the form for your tax refund, please click here

Regards,Internal Revenue Service

3/13/2006

HOW DO THEY GET MY INFORMATION

SAMPLE OF PHISHING EMAIL

From: clearings174@gmail.com

Transaction is completed. $2007 has been successfully transferred.
If the transaction was made by mistake please contact our customer service.
Payment receipt is attached.

*** This is an automatically generated email, please do not reply ***
Bank of America, N.A. Member FDIC. Equal Housing Lender Opens in new window

HOW DO THEY GET MY INFORMATION
SAMPLE OF PHISHING EMAIL

Bank of America

For your security, access to Online Banking has been locked because the number of attempts to sign in exceeded the number allowed.
To regain access to your internet banking, Please update and select the Reset Account link. below.

We will review the activity on your account with you and upon verification, we will remove any restrictions placed on your account.

To access and activate your account, simply click the link below.

www.bankofamerica.com/onlinebanking/index.php?id=zxdj9b32wx

The entire activation should take only 5 minutes of your time. Please complete the activation by now.

Thank you for using Online Banking.
Bank Of Ameria Alerts

If you no longer wish to receive these e-mails, please click on this link:
www.bankofamerica.com/onlinebanking/index.php?id=deactivate

HOW DO THEY GET MY INFORMATION

How to fake an ATM

Next time you use a bank machine, check closely to make sure it's the real thing. Cops in San Francisco report that thieves are now installing fake overlays on banking ATMs. The fakes swallow your card, record your PIN, and report that they're out of service; the thieves show up later to remove the fake overlay and harvest the cards and collected PINs.

HOW DO THEY GET MY INFORMATION

Ordinary ATM?

Skimming equipment installed

Hidden PIN recording camera

Camera records PIN as keyed in

HOW DO THEY GET MY INFORMATION

- **ATM Scam -** Wireless, shoulder surfing, cell phone video
- **Buying your information**
  - AOL employees fired selling 250,000 customers information
- **Computer information stolen**
  - Ameriprise financial laptop stolen - 225,000 customers data lost
  - VA has laptop stolen with 2.3 million military personal information stolen, including Social Security numbers

HOW DO THEY GET MY INFORMATION

- IRS Laptop stolen from Mpls office w/over 100,000 people/business
- information on it.

- Boston Globe & Worchester Telegram & Gazette deliver newspapers
- w/240,000 subscribers information list

- Ernest & Young – 243,000 customers of Hotels.com data on stolen laptop from
- Employee's car in Texas

- Laptop missing from Twin Cities blood bank – 268,000 customers data

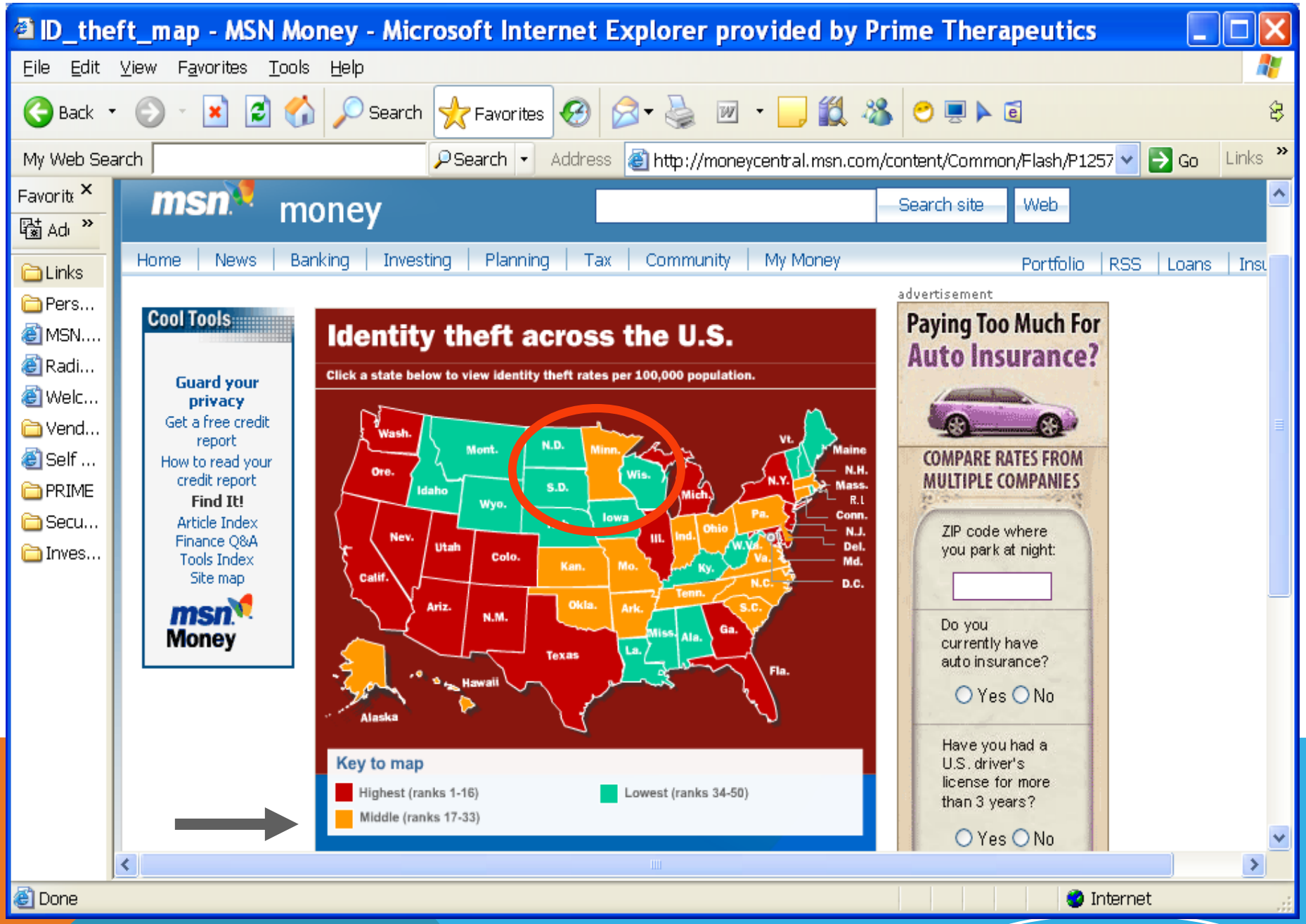
- 3.3. million student loan information stolen from MN company

HOW DO THEY GET MY INFORMATION

- Simply ask for it on the phone – SCAM
  - Grandparent call from outside U.S. – 'Send money- don't tell Mom & Dad!"
- File tax return with refund in your name, different address
  - 4/12/13 – Two charged in Tampa, FL using stolen ID's
- Steal from home
  - Family/In-Home workers
- Couple fleeced of $400,000 by financial planner
- Rental/Real Estate Scams
- Mystery/Secret Shopper
- New York Relief Fraud
- Computer Pop-Up ad's offering FREE AV Software
- Gift cards forged
- Threaten/Guilt – Jury Duty, Lawsuit, Arrest Warrant

HOW DO THEY GET MY INFORMATION

- You Tube Videos – can contain/download malware
- Using children's SSN that do not work yet
- Facebook
  - People post when on vacation, how long, etc.
  - Think their data is private/protected
- TWITTER accounts
- Blog Sites
  - Posting detailed information about yourself
- Text messaging
  - Is NOT secure
- E-mail
  - Like reading a post card found on the ground



MN ranks 28th, WI 37th, IA 45th, ND 49th, SD 50th

WHAT TO DO IF YOU ARE A VICTIM

- File a police report – a MUST DO
  - Get the file number
- Place a Fraud Alert on all three credit reports-review carefully
  - Contact three primary credit agencies:
    - Equifax – 1-800-525-6285, www.equifax.com
    - Experian – 1-888-397-3742, www.experian.com
    - TransUnion – 1-800-680-7289, www.tuc.com
      - Innovis – 1-800-540-2505, $3-1st 12 months - $11 thereafter for small business
      - https://www.innovis.com/InnovisWeb/pers_orderCreditReport.html
  - Request a freeze on all 3 credit reports
    - $5.00 for each freeze/thaw – no limit on how often freeze/thaw
    - Freeze may only be good for 12 months
  - Obtain all 3 credit reports once a year – 1-877-322-8228 or www.annualcreditreport.com

WHAT TO DO IF A VICTIM

- Close all accounts that have been tampered with
- File complaint with the FTC – recommend follow up to ensure they received it
  - www.ftc.gov/idtheft
  - Phone: 1-877-438-4338
  - Mail: Identity Theft Clearinghouse, Federal Trade Commission, Washington, DC 20580
- Log everything
  - Keep notes of phone conversations, send mail certified, keep receipts of expenses, your time

HOW TO PROTECT YOURSELF

- Guard your SSN
- Don't carry credit cards you don't need
- Limit number of credit card accounts to 2 or 3
- Don't use mail boxes for sending mail
- Men - carry wallet in your front pocket
- Purses go over both shoulders, zipped shut
- Be aware of people around you at ATM machines
- Do not give out any personal information over the phone or in email unless you absolutely know who you're giving it to (you contact THEM)

HOW TO PROTECT YOURSELF

- Don't believe phone solicitors
- Add yourself to the National Do Not Call list:
  - www.donotcall.gov or 1-888-382-1222
  - Expires every 5 years
- Close all unnecessary accounts
- Don't pre-print phone number on checks
- Have checks mailed to a PO Box or pick them up at the bank
- Before traveling out of country tell your Credit Card Company where and how long you will be gone

HOW TO PROTECT YOURSELF

- Keep important documents secure
  - SSN card, birth/marriage certificates, wills, etc.
  - Fire resistant container or Bank Safety Deposit Box
- Pay bills via internet is okay
  - Address MUST start with ***https***, NEVER http
- Review monthly statements for discrepancies
  - Immediately challenge them
- Buy a crosscut shredder & shred all monthly statements
  - No need to keep copies of bills, almost all are available on-line
- All medical information must be protected the same as financial
- Opt out of pre-approved credit offers
  - 888-567-8688 / (888)5OPTOUT, or # on solicitation
- Be aware of what you post on or send via the internet or cell phone
- Obtain all 3 credit reports once a year – 1-877-322-8228 or **www.annualcreditreport.com**

HOW TO PROTECT YOURSELF

- Install operating system updates on your cell phones when prompted or they become available
- Password protect your phone
  - Recommended standard - Change password every 72 days
- Use metal lined wallets for credit cards
- Expect to be a victim
- Support employees that become victims

HOW TO PROTECT YOURSELF

Service to protect you – Not Necessary

- LifeLock – www.lifelock.com
  - Provides service you can do yourself for FREE
    - $10.00 per month per adult
  - Internet Review - http://identity-theft-protection-services-review.toptenreviews.com/
  - LifeLock settles 12 million dollar lawsuit http://abclocal.go.com/wpvi/story?section=news/consumer&id=7321200
- FreeCreditScore.com
  - Owned by Experian Consumer Direct, a subsidiary of the credit bureau Experian
  - 2005 sued by FTC

    2006 sued by Florida State Attorney General

RESOURCES

Recognize ID Theft Scams:
http://idtheft.about.com/od/preventionpractices/ss/phishing_scams.htm

Federal Trade Commission:
http://www.ftc.gov/bcp/edu/microsites/idtheft/become-a-partner.html

http://www.ftc.gov/bcp/edu/microsites/idtheft/video/avoid-identity-theft-video.html

Privacy Rights Clearinghouse: www.privacyrights.org

MSN Money: www.moneycentral.msn.com

Minnesota Attorney General's Office: www.ag.state.mn.us

ID Theft Prevention & Survival:
http://www.identitytheft.org/

RESOURCES

Internet Crime Complaint Center:
http://www.ic3.gov/default.aspx

FBI - http://www.fbi.gov/

New York Times – www.nytimes.com/

Star Tribune: www.startribune.com/

SLATE
http://www.slate.com/blogs/future_tense/2013/03/26/andrew_weissmann_fbi_wants_real_time_gmail_dropbox_spying_power.html

QUESTIONS?????

Kelley P. Archer, CISSR

issaman@mchsi.com